

REMARKS

With this Response, Applicants respectfully request that claims 12, 16-32, and 44 be canceled without prejudice. Furthermore, claims 1-3 and 33-35 are amended. Therefore, claims 1-5, 10-11, 13-15, 33-37, 42-43, and 45-47 are pending.

REJECTIONS UNDER 35 U.S.C. § 101

Claims 33-47

Claims 33-47 were rejected under 35 U.S.C. § 101 as being directed to non-patentable subject matter. More particularly, these claims were rejected as being directed to "an electronic signal," which is deemed a form of energy, and thus not within the statutory categories of patentable subject matter. Applicants respectfully traverse. Applicants' claims are directed to "An article comprising: a tangible **storage medium having a plurality of machine accessible instructions stored thereon**, wherein when the instructions are executed...." Applicants respectfully request clarification as to how the Office can possibly interpret such claim language as "an electronic signal". It is irrelevant what is stated in paragraph [0105] if the claim does not read on a form of energy, which it does not. The argument in the Office Action at page 2 is insufficient to support a rejection of the claims on the basis of 35 U.S.C. § 101. The claims are directed to an article, which is one of the four statutory categories of patentable subject matter. The rejection in the Office Action is defective, and Applicants respectfully request that it be withdrawn.

REJECTIONS UNDER 35 U.S.C. § 102

Claims 1-5, 10-13, 15, 33-37, 42-45 and 47

These claims were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2005/0063544 of Uusitalo et al. (hereinafter "Uusitalo"). Claims 12 and 44 are canceled herein, rendering rejection of these claims moot. The remaining claims are not anticipated by the cited references for at least the following reasons.

Independent claims 1 and 33 as amended herein recite, among other things not disclosed or suggested by the references, features directed to generating a master secret by **mixing a pre-master secret and a cryptographic hash of a platform configuration**.

The Office Action relies on the mention in Uusitalo as disclosing the use of multiple keys in authentication. Even assuming for the sake of argument that the reference can be interpreted as disclosing the use of multiple keys in authentication, which Applicants do not concede, the Office Action has failed to point to anything that discloses or suggests a platform configuration value, in contrast to what is recited in Applicants' claims. The Office Action points to paragraph [0048] of the reference, which makes reference to "taking a hash of the PMK." Applicants point out that taking a hash of a PMK (Pre-Master Key) by itself fails to disclose or suggest mixing a pre-master secret with other information. The PMK as disclosed in Uusitalo appears to be used solely for purposes of decrypting exchanged messages (see, for example, paragraphs [0049] and [0050]), and is not mixed with anything, in contrast to what is recited in Applicants' claims. Much less is there anything to suggest a platform configuration and mixing a pre-master secret with a cryptographic hash of the platform configuration. Thus, the cited reference fails to disclose or suggest at least one feature of the claimed invention, and so fails to anticipate the invention as recited in Applicants' claims.

REJECTIONS UNDER 35 U.S.C. § 103

Claims 14 and 46

Claims 14 and 46 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Uusitalo in view of U.S. Patent No. 4,649,233 of Bass et al. (hereinafter "Bass"). Bass is recited as disclosing halting an authentication process if problems arise during authentication. Assuming for the sake of argument that Bass discloses what is asserted in the Office Action at pages 8 to 9, which Applicants do not concede, the reference is not cited as curing, and indeed does not cure the deficiencies of Uusitalo discussed above. Whether alone or in combination, the cited references fail to disclose or suggest at least the feature of a platform configuration, or more significantly of mixing a pre-master secret with a cryptographic hash of the platform configuration, in contrast to what is recited in Applicants' claims. Therefore, the references fail to support a rejection of the independent claims upon which these claims depend, and so likewise fail to support a rejection of these claims.

CONCLUSION

For at least the foregoing reasons, Applicants submit that the rejections are overcome, and respectfully requests that the rejections be withdrawn. Therefore, all pending claims are in condition for allowance, and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application.

Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: June 17, 2008

/Vincent H. Anderson/
Vincent H. Anderson
Reg. No. 54,962
Attorney for Applicant

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below.

Date: June 17, 2008

/Katherine Jennings/
Katherine Jennings